LKA 543
Hamburg

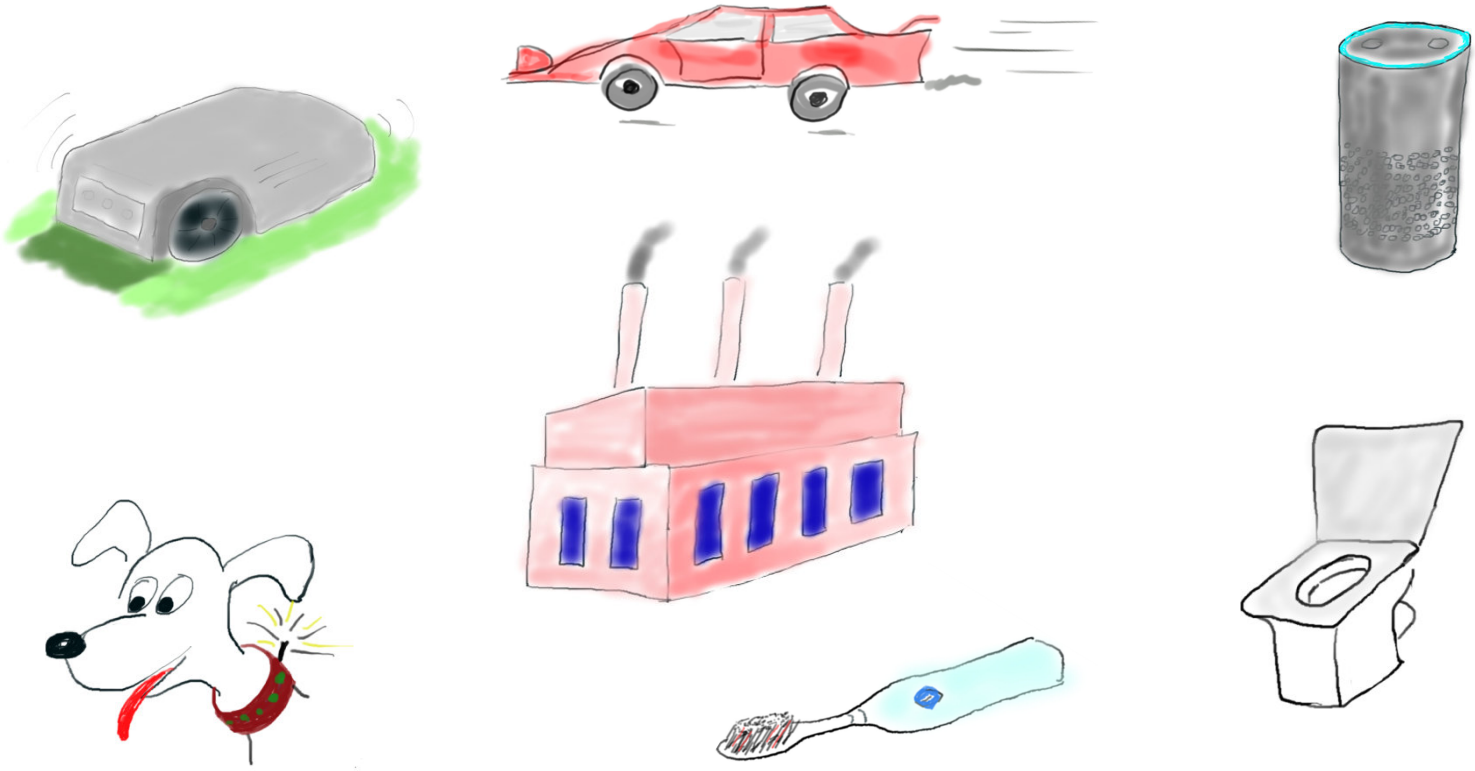
Cybercrime

Aktuelle Phänomene und Handlungsempfehlungen der Polizei Hamburg

Agenda

- Einleitung ins Thema
- CEO-Fraud / Payment Diversion Fraud
- Malware spez. Ransomware
- DDoS und weitere Angriffsfelder
- Polizei / Ermittlungen
- Maßnahmen
- Fazit

Digitalisierung



Tätertypen

§ LKA 541

§ LKA 542

§ LKA 543

CEO-Fraud 2015/2016

Sehr geehrte Frau M.,

ich kann doch in einer streng vertraulichen Finanzangelegenheit auf Ihre Unterstützung zählen. Unser Unternehmen plant eine Expansion in den asiatischen Geschäftsraum und wird hierzu eine existierende Firma übernehmen. Wie Sie sicher verstehen können, ist diese Transaktion streng geheim. Aus diesem Grunde und zu Dokumentationszwecken für die Bafin darf die gesamte Kommunikation mit mir ausschließlich per Mail erfolgen.

Mit der Abwicklung wurde das Schweizer Notariat E. betraut. Der Rechtsanwalt und Notar Dr. E. wird sich morgen telefonisch bei Ihnen bezüglich der Details melden.

Bitte bereiten Sie alles für eine entsprechende Auslandsüberweisung vor.

Ich weiß, dass ich mich auf Sie verlassen kann.

Mit freundlichen Grüßen

Dr. W., CEO

CEO-Fraud 2017/2018

Guten Marion,

Was ist unser Bankguthaben?

Können wir heute 70T bezahlen?

Gruß

Thomas Meier

Geschrieben von iPhone

CEO-Fraud 2017/2018

OK. Bitte zahlen

Account Name: xxxx

Bank Name: xxxx

IBAN: xxxx

Bank Address: xxx

Zweck der Bezahlung: Neuer technischer Maschinenkauf

69.359,- Euro

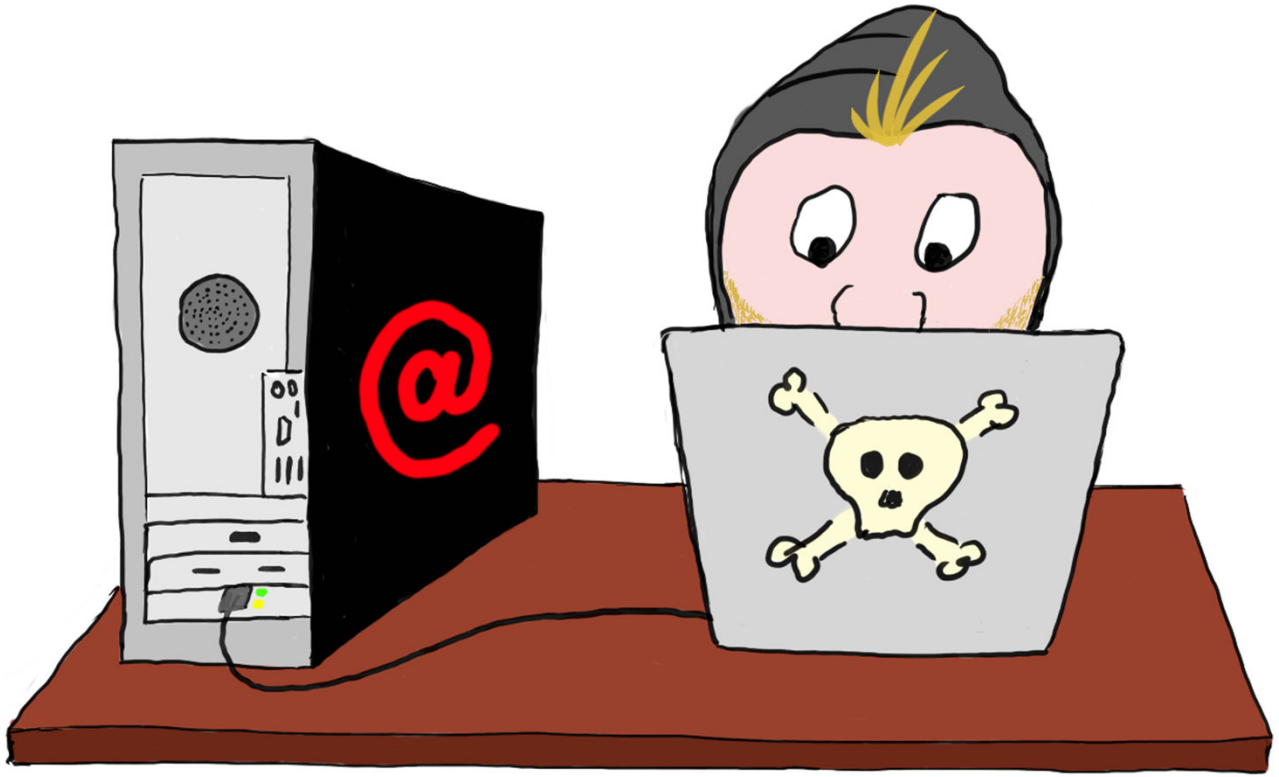
Senden Sie mir eine Zahlungsbestätigung

Gruß

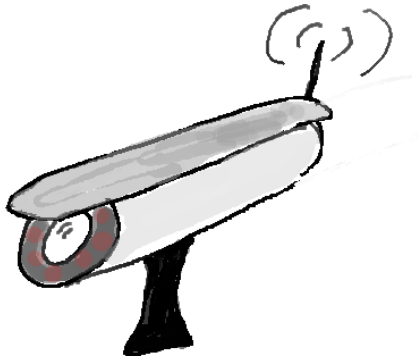
Thomas Maier

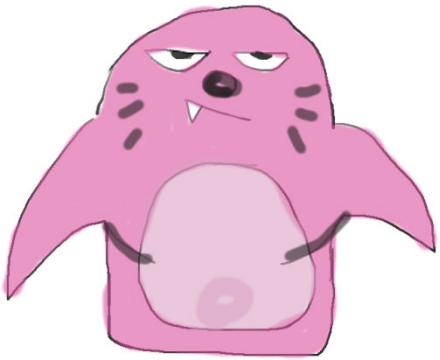
Gesendet von iPhone

Mail-Kompromittierung



Informationsbeschaffung





Maßnahmen

- Awarenessmaßnahmen bei den Mitarbeitern
- Technische Maßnahmen / Passwortsicherheit
- Klare Abläufe definieren
- Strategien der Geschäftsführung

Malware

Malware

Fall 1

Ein Angestellter öffnet eine Bewerbungsmail auf seinem Arbeitsplatz-PC. Aufgrund eines mangelhaften Rechtemanagements kann die enthaltene Schadsoftware sämtliche Netzwerkfreigaben und das Backup des Unternehmens verschlüsseln. Die Firma ist gezwungen das Lösegeld zu zahlen, da ansonsten das Fortbestehen gefährdet ist.

Fall 2

Ein Angestellter erhält auf seinem privaten Smartphone eine Email mit einem Dateianhang, welchen er nicht öffnen kann. Er loggt sich vom Firmenrechner aus in seinem privaten Email-Konto ein und öffnet den Dateianhang. Von dem Rechner verbreitet sich die im Anhang enthaltene Verschlüsselungssoftware auf dem gesamten Serversystem des Unternehmens. Es kommt zum Totalausfall der Produktion wodurch pro Tag ein Schaden im hohen 6-stelligen Bereich anzunehmen ist.

Fall 3

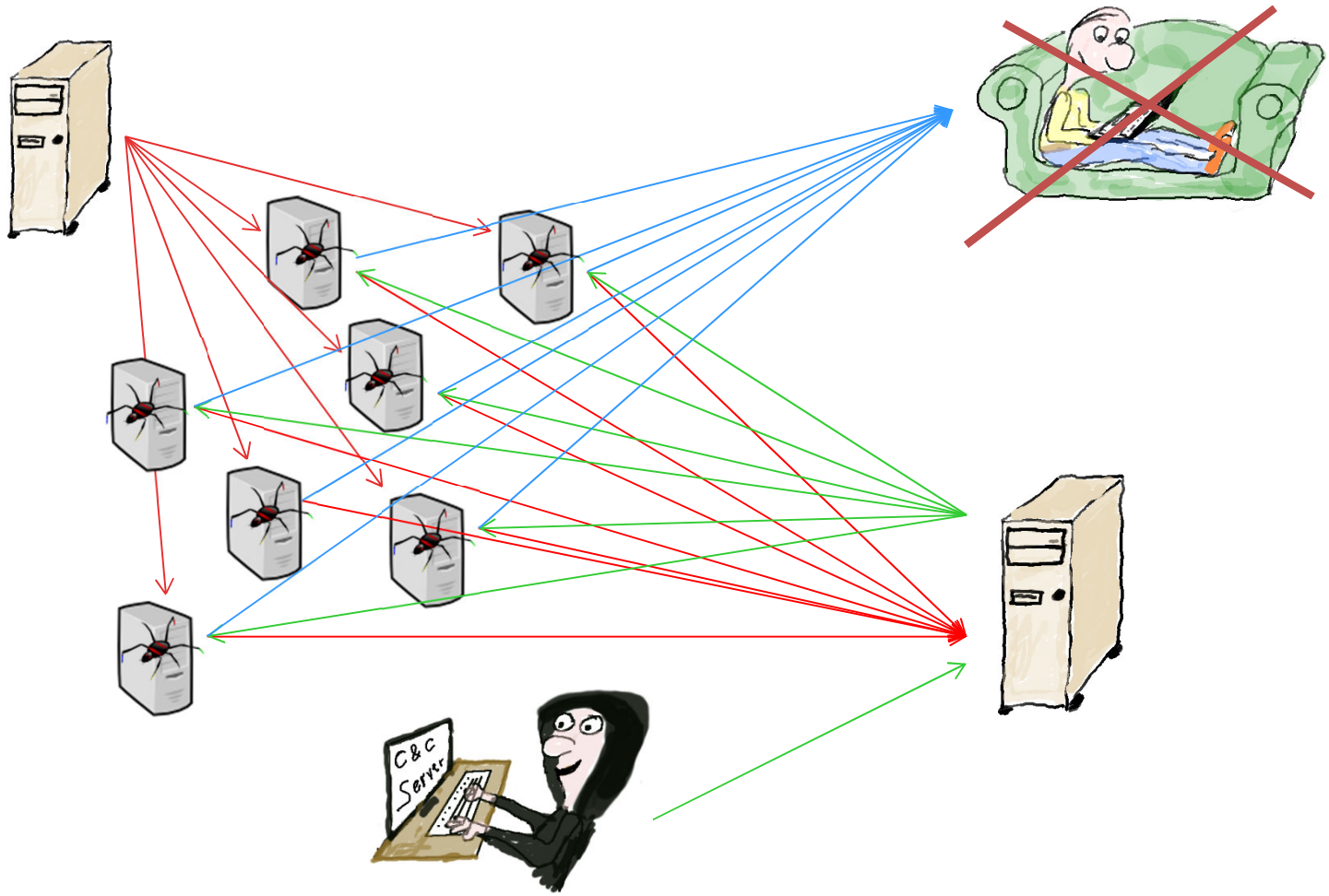
Über einen Updateprozess wird eine Schadsoftware auf einem Unternehmenscomputer eingespielt. Diese verbreitet sich unter Ausnutzung von Sicherheitslücken auf allen erreichbaren Rechnern im gesamten Firmennetzwerk und verschlüsselt zu einem vordefinierten Zeitpunkt sämtliche Systeme.

Maßnahmen

- Awarenessmaßnahmen bei den Mitarbeitern
  - Problem „Gutgläubigkeit“
  - Problem „Vertrauen in die IT“
- Regelmäßige Datensicherungen
- (vernünftiges) Rechtemanagement
- Antivirensoftware auf allen Systemen

DDoS

DDoS



DDoS

Hi!

If you dont pay 5 bitcoin until 1. february you will be hardly ddosed!
Our attacks are super powerfull (Mirai botnet). And if you dont pay until 1. february ddos attack will start and price to stop will double!
We are not kidding and we will do small demo now on just one of your servers xxx.xx.xxx.xxx to show we are serious. It will not be strong, we dont want damage now we hope you cooperate, just small flood to show we are not hoax.
Pay and you are safe from us forever. Ignore, you go down longtime and price go up.
OUR BITCOIN ADDRESS: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
Dont reply, we will ignore!
Pay and we will be notify you payed and you are safe.

Cheers!

Maßnahmen

- Risikobewertung
  - ggf. betroffene Geschäftsbereiche?
  - Verluste (z.B. Onlineshops)
- Kontaktaufnahme mit ISP
- ggf. Beratung durch speziellen Anbieter

weitere Angriffsfelder

Bitcoin

Ursachen für Erfolge der Täter

- Der Glaube, dass einem nichts passiert
- IT-Sicherheit als Zustand betrachten
- Unzureichende Awarenessmaßnahmen
- Unzureichendes Rechtemanagement
- Unzureichende / keine Backuplösungen
- Komplexität der Unternehmensstruktur
- Komplexität der Software
- usw.

Polizei

Ermittlungsmöglichkeiten

- CEO/Payment-Diversion-Fraud
  - E-Mailadresse?
  - IP-Adresse aus Header?
  - ggf. Rufnummer?
  - ggf. Bankverbindung?

- Ransomware / DDoS / Erpressung
  - E-Mailadresse?
  - IP-Adresse aus Header?
  - Bitcoin-Adresse?

Ermittlungen 2020?

- Neue Kriminalitätsfelder
  - Industrie 4.0
  - „Smart“ City / Car / Home usw.
  - weitere Verlagerung klassischer Kriminalität
- Weniger Ermittlungsmöglichkeiten
  - Verschlüsselung von Geräten
  - Verschlüsselung von Kommunikation
  - Verschlüsselung von Webseiten

Incident Response

Planen Sie den Sicherheitsvorfall bevor er passiert!

- Dokumentieren Sie Ihre IT-Struktur.
- Wer ist der verantwortliche Ansprechpartner?
- Woher bekommt man Bitcoins?
- Analyse des Angriffs (Kosten/Nutzen)?
- Polizei einschalten: ja / nein?
- Umgang mit Medien / Presse
- ggf. Umgang mit Kunden
- Meldepflichten?
- usw.

IT-Sicherheitsanalyse

Grundlegende Fragen:

- Welche Daten besitzen wir?
- Was sind unsere wichtigsten Daten?
- Wo liegen diese Daten?
- Wer hat Zugriff auf diese Daten?
- Welche Maßnahmen wurden bereits ergriffen, um diese Daten zu schützen?
- Sind alle digitalen Geschäftsprozesse bekannt und definiert?
- usw.

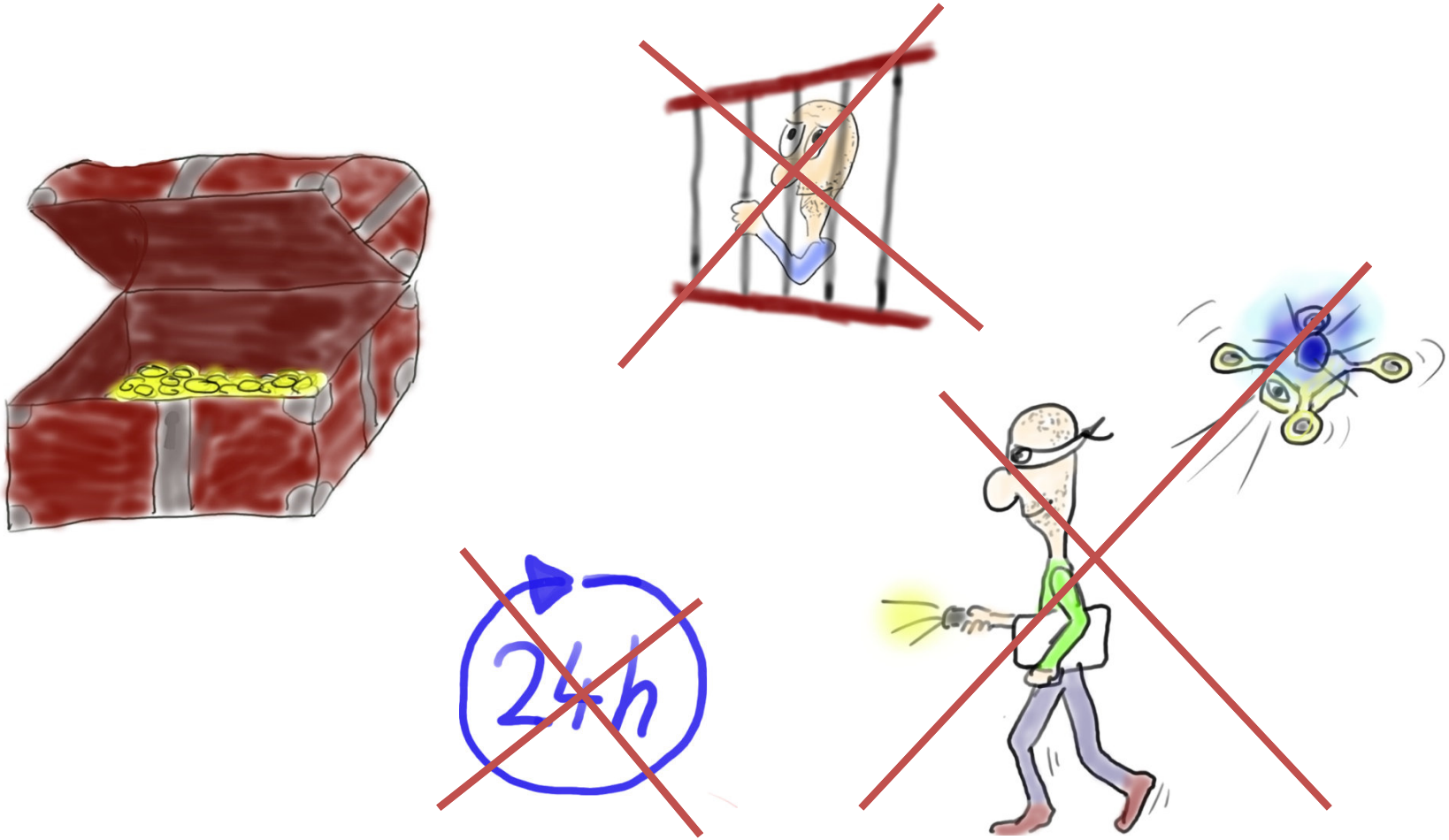
Bedenkenswertes

Versicherung?

go-digital

EU-DSGVO?

Kriminologie

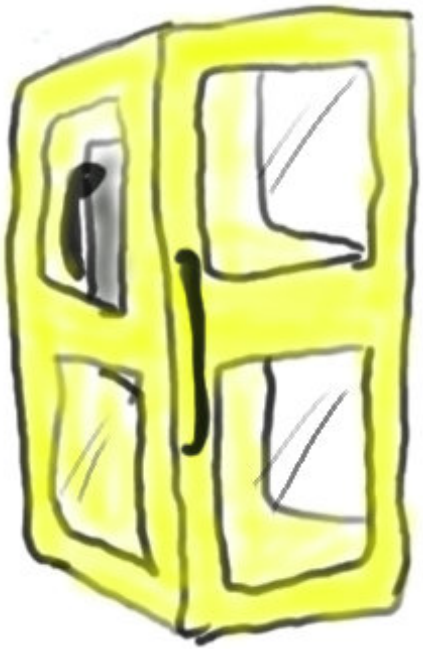


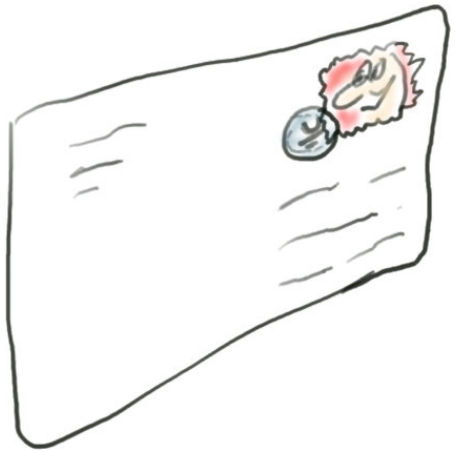
Gewinne bei Cybercrime

Straftat/Gewinn		Ursache
CEO-Fraud	à	User
Malware	à	User
Betrug	à	User
DDoS	à	User

Stichwort: User-Prävention!

Entwicklung 1987 - 2017





Kommunikation 1987

Entwicklung 1987 - 2017

Kommunikation 2017

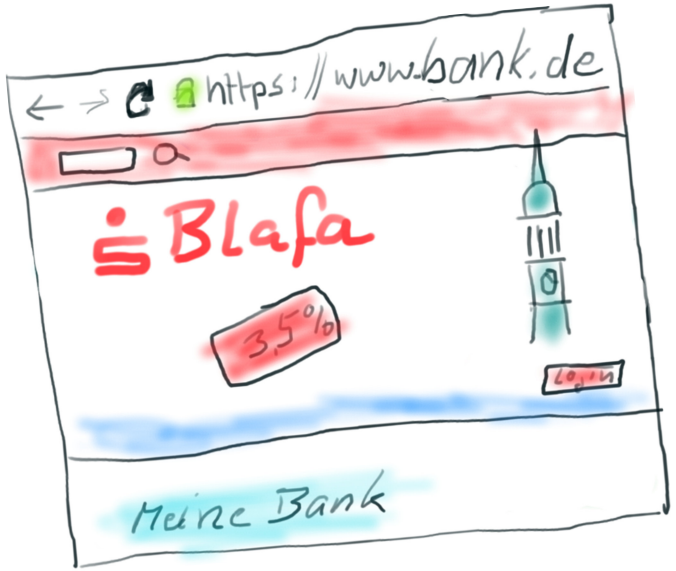
Entwicklung 1987 - 2017

Geld und Waren 1987

Entwicklung 1987 - 2017

amazon

ebay



Geld und Waren 2017

Entwicklung 1987 - 2017

Informatikpflichtstunden 1987

(in Hamburg)

0

Entwicklung 1987 - 2017

Informatikpflichtstunden 2017
(in Hamburg)

0

zum Vergleich (Klasse 5-10): Theater: 76
Musik und Kunst je: 152, Sport: 684

Bildung

Die Medienerziehung, die Erziehung zur Medienmündigkeit und zu einem vernünftigen Umgang mit Medien, muss in den Elternhäusern stattfinden.

Josef Kraus, Präsident Deutscher Lehrerverband,
Interview in der Tagesschau vom 19.04.2017

Fazit

Es wird nicht besser!

Vielen Dank für Ihre Aufmerksamkeit

Polizei Hamburg
LKA 543
Bruno-Georges-Platz 1
22297 Hamburg
Tel: +49(0)40 4286-75455
Fax: +49(0)40 4279-99141
E-Mail: zac@polizei.hamburg.de